IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK,

*Plaintiff*

v.

SYMANTEC CORPORATION,

*Defendant*

Civil Action No. 3:13-cv-00808-JRS

**JURY TRIAL DEMANDED**

# SYMANTEC CORPORATION'S RESPONSIVE CLAIM CONSTRUCTION BRIEF

## TABLE OF CONTENTS

# TABLE OF AUTHORITIES

**Page(s)**

## Cases

**Statutes**

# I. INTRODUCTION

Columbia's proposed constructions and the arguments presented in its opening brief ignore the intrinsic record of the asserted patents in an attempt rewrite the asserted claims to cover subject matter expressly distinguished in the specification or prosecution history. For instance, the '084 and '306 patents disclose prior art intrusion detection systems that "detect the effects or behavior of malicious software." *See* Dkt. No. 107-7 ('084 patent) at 2:22-25. The patents then contrast those systems with the invention, *i.e.*, anomaly detection systems that "do not operate by looking for malicious activity directly," but instead "look for deviations from normal activity." *Id*. at 2:34-37 and 7:47-49. Columbia drafted the claims of the '084 and '306 patents consistent with this distinction, specifically requiring a "model of ***normal*** computer system usage" and "detecting deviations from ***normal*** computer system usage" to identify "an anomaly." *See*, *e.g.*, '084 patent at claim 1. Columbia then defended these claims during prosecution against prior art that discloses—in Columbia's own words—a system where "an attack is predicted if it conforms with attacks which were observed during model training." *See* Dkt. No. 107-30 ('084 patent prosecution history) at COL00144299. Now, in litigation, Columbia regrets these decisions and hopes to rewrite its claims to cover subject matter that it expressly distinguished from the claimed invention. Specifically, Columbia seeks to construe the claimed "model of ***normal*** computer system usage" broadly to encompass models that predict an attack if it conforms with attacks observed during model training.

Similarly, the '544 and '907 patent specifications describe three distinct ways to perform a technique called feature extraction: the first uses "byte sequences," the second uses "resource information," and the third uses "encoded strings." Columbia purposefully drafted its claims to cover only the "byte sequence" method of feature extraction. *See*, *e.g.*, Dkt. No. 107-3 ('544 patent) at claim 1. But now, in litigation, Columbia asks the Court to broaden the claims beyond the "byte sequence" method, in order to encompass the other feature extraction methods that Columbia did not claim.

The Court should reject Columbia's litigation-driven efforts to redraft its claims, and instead construe the disputed terms consistent with their ordinary meaning in the context of the intrinsic record of which they are a part.[1]

## II. **‘544 AND ‘907 PATENTS**

### A. **"byte sequence feature" and "feature"**

| Symantec's Proposed Construction | Columbia's Proposed Construction |
|---|---|
| "feature": a property or attribute of data which may take on a set of values<br>"byte sequence feature": feature that is a representation of machine code instructions of the executable | If the Court believes the term should be construed:<br>"byte sequence feature": property or attribute of a sequence of bytes, which may take on a set of values |

The ‘544 and ‘907 patents describe three distinct methods for extracting features from executable attachments. The distinct methods extract ***either*** (1) "byte sequence" features, (2) "resource information" features, ***or*** (3) "encoded string" features. *See* Dkt. No. 107, Symantec Corporation's Opening Claim Construction Brief (Symantec Op. Br.) at 3-5. The patents explain that only the first of these three methods results in extraction of "byte sequence features." *See*

[1] In support of its opening brief, Columbia submitted the 36-page Declaration of Douglas Szajda, *see* Dkt. No. 106-1 (Szajda Decl.). Columbia characterized the declaration as a "tutorial," intended to be read before reviewing Columbia's brief. *See* Dkt. No. 106, Columbia's Opening Claim Construction Brief (Columbia Op. Br.) at 1. The parties did not seek to submit a tutorial, nor has the Court requested one. And, for the most part, the declaration is not a tutorial at all, but instead a legal brief of claim construction arguments. The declaration, therefore, is a transparent effort to evade the page limits imposed by the local rules, and Symantec requests that the Court disregard it. Additionally, as discussed herein, the declaration is extrinsic evidence containing conclusory arguments that contradict the intrinsic record, so the Court should disregard it as a matter of law. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1318 (Fed. Cir. 2005) (*en banc*) (conclusory expert testimony is unhelpful, particularly where it contradicts the intrinsic record).

‘544 patent at 6:7-22.

The ‘544 and ‘907 patents describe the byte sequence feature extraction method as follows:

> In the exemplary embodiment, hexdump was used in the feature extraction step. Hexdump, as is known in the art (Peter Miller, “Hexdump,” on line publication 2000, http://gd.tuwien.ac.at/softeng/Aegis/hexdump.html which is incorporated by reference in its entirety herein), is an open source tool that transforms binary files into hexadecimal files. ***The byte sequence feature is informative because it represents the machine code in an executable***. After the “hexdumps” are created, features are produced in the form illustrated in FIG. 2 in which each line represents a short sequence of machine code instructions. In the analysis, a guiding assumption is made that similar instructions were present in malicious executables that differentiated them from benign programs, and the class of benign programs had similar byte code that differentiated them from the malicious executables. Each byte sequence in the program is used as a feature.

‘544 patent at 6:7-22 (emphasis added). The patents state unequivocally that the byte sequence feature extracted via this method “represents the machine code in an executable,” and Symantec’s proposed construction accounts for this description. *See id*. at 6:12-14; *see also id*. at 13:24-26 (“This byte sequence is useful because it represents the machine code in an executable.”).

The ‘544 and ‘907 patents contrast byte sequence feature extraction with resource information extraction—also referred to as binary profiling—which the specification describes as an “alternative[]” employed in “another embodiment”:

> [A]nother approach to feature extraction is to ***extract resource information*** from the binary that provides insight to its behavior, which is also referred to herein as “binary profiling.”

*Id*. at 6:26-29 (emphasis added).

> It is understood that the ***feature extraction step described herein is alternatively performed with a binary profiling method in another embodiment***, as described above and illustrated in FIGS. 3-4, and with a GNU strings method, also described above and illustrated in Table 1. In these embodiments, the step of calling the routine hexScan in scanAttachments is replaced by calls to routines that perform the binary profiling or GNU strings analysis.

*Id*. at 13:29-37 (emphasis added). Resource information extraction, therefore, is a different extraction method targeted to different features than the disclosed byte sequence feature extraction method. Resource information extraction is ***not*** a different way to extract the same type of features, as Columbia contends. *See* Columbia Op. Br. at 7.

This understanding is confirmed in the intrinsic record, which describes features extracted from each method as different classes of features—not different examples of a single class. *See* Dkt. No. 107-4, U.S. Provisional Application No. 60/308,622 at COL00007540. The '544 and '907 patents claim priority to and incorporate by reference the '622 application, which includes Section 4, titled "Feature Extraction." *See id*. Subsection 4.1 discusses the resource information extraction method. *See id*. at COL00007541 ("To extract resource information from Windows executables we used GNU's Bin-Utils."). And Subsection 4.3 discusses the byte sequence feature extraction method. *See id*. at COL00007542 ("Byte sequences are the last set of features that we used over the entire 4,266 member data set."). Section 4 introduces the resource information method and byte sequence method as distinct techniques for extracting different features representing different information:

> In this section we detail all of our choices of features. ***We statically extracted different features that represented different information within each binary***. These features were then used by the algorithm to generate detection models

*Id*. at COL00007540 (emphasis added). The '622 application further confirms that Symantec's proposed construction is correct because it distinguishes the byte sequence feature extraction method as superior to the resource information extraction method. *Id*. at COL00007542 (explaining that a byte sequence feature advantageously "represents the machine code in an executable instead of resource information like libBFD features.").

If Columbia's position were correct, Columbia would be able to identify a disclosed embodiment that describes a "resource information" feature as a "byte sequence" or "byte sequence feature." Columbia cannot do that, because no such description exists.[2]

The Federal Circuit recently encountered this exact situation in *Abbvie Inc. v. The Mathilda and Terence Kennedy Institute of Rheumatology Trust*, No. 2013-1545, -- F.3d --, 2014 WL 4100584 (Fed. Cir. Aug. 21, 2014). The claims in *Abbvie* related to methods of treating rheumatoid arthritis by "co-administering" two drugs. *Id.* at *1. The patentee appealed on the grounds that the district court improperly limited its construction of "co-administering" to three methods of administration, arguing that the specification disclosed a fourth method—"administration of the antibody alone after discontinuing the administration of methotrexate." *Id.* at *7. The Federal Circuit rejected the patentee's argument and affirmed the district court, explaining that "[t]he specification never uses the term 'co-administering' to refer to patients who only received the antibody after discontinuing treatment with methotrexate." *Id.* Here, the intrinsic record of the '544 and '907 patents never refers to resource information features as an example of the claimed "byte sequence feature," and in fact the specification distinguishes one from the other. *See* '544 patent at 13:29-37. Accordingly, it would be improper to construe "byte sequence feature" to encompass resource information features.

Columbia's complaints appear directed not to Symantec's inclusion of machine code instructions in its "byte sequence feature" construction, but rather to the inclusion of ***only*** machine code instruction information, and not all other file contents. *See* Columbia Op. Br. at 7 ("The patent discusses extracting a byte sequence feature based on all elements in an executable, not just instructions."); *id.* at 8 ("the inventors emphasize the desire to capture all information in

[2] Columbia's citation to the "Summary" of the '544 and '907 patents is not to the contrary. *See* '544 patent at 3:37-40. That section merely parrots the claim language and does not describe any actual embodiment. *See* Section II.B below.

the program when creating features.”). Columbia argues that Symantec’s construction cannot be correct, because the inventors expressed a desire to utilize a method that analyzed all aspects of a file and not a single portion. *See id*. This complaint is puzzling, because Columbia’s proposed construction does not require the byte sequence feature to include features representing *any* particular file content, let alone all file content.

Columbia’s construction also would render the words “byte sequence” in “byte sequence feature” superfluous. Every attribute or property of a file could be considered an attribute or property of a sequence of bytes, because all files are composed entirely from a sequence of bytes. *See* ‘544 patent at 13:18-22 (representing a “binary file[]” as a “byte sequence.”). Had Columbia wanted its claims to cover all types of file features rather than just byte sequence features, it could have done so by simply referring to a “feature” instead of a “byte sequence feature” in the claim. *See Haemonetics Corp. v. Baxter Healthcare Corp.*, 607 F.3d 776, 781 (Fed. Cir. 2010) (“Patent claims function to delineate the precise scope of a claimed invention and to give notice to the public, including potential competitors, of the patentee's right to exclude. This notice function would be undermined, however, if courts construed claims so as to render physical structures and characteristics specifically described in those claims superfluous.”) (internal citation omitted). Columbia limited the claims to a particular type of feature, and the Court should deny its effort to broaden the claims and thereby undo this choice.

### B. “wherein extracting said byte sequence features from said executable attachment comprises creat[ing/e] a byte string representative of resources referenced by said executable attachment”

| Symantec’s Proposed Construction | Columbia’s Proposed Construction |
|---|---|
| Indefinite | If the Court believes the term should be construed: wherein the byte sequence feature includes a byte string representative of resources referenced by the executable attachment |

According to the inventors of the ‘544 and ‘907 patents, “resource information” features and “byte sequence features” are “***different features*** that represented ***different*** information contained within each binary.” *See* ‘622 application at COL00007540 (emphasis added). But the limitations of claims 1 and 16 of the ‘544 patent at issue here ***combine*** these feature extraction methods, requiring that extracting byte sequence features comprises creating a byte string representative of resources referenced by the executable. *See*, *e.g.*, ‘544 patent at claim 1. A claim limitation that on its face may appear straightforward may nevertheless be indefinite if the limitation does not make sense when read in the context of the specification. *See Allen Eng’g Corp. v. Bartell Industries*, 299 F.3d 1336, 1349 (Fed. Cir. 2002) (“Where it would be apparent to one of skill in the art, based on the specification, that the invention set forth in a claim is not what the patentee regarded as his invention, we must hold that claim invalid under § 112, paragraph 2”). That is the case here.

Columbia’s reliance on the specification of the ‘544 and ‘907 patents to support its position is misplaced. Columbia cites a portion of the “Summary of the Invention,” which states, “According to another embodiment, extracting the byte sequence features from the executable attachment may comprise creating a byte string representative of resources referenced by said executable attachment.” ‘544 patent at 3:37-40. This “summary” merely parrots the claim language, without providing any description of how a byte string representative of resources referenced by an executable attachment would be created. Notably, the “embodiment” that this statement purportedly “summarizes” does not appear in the “Detailed Description of Exemplary Embodiments.” *See id*. at 4:52 *et seq*. In fact, the descriptions of the preferred embodiment teach the opposite: that byte sequence feature extraction and creation of byte strings representative of resources are two mutually exclusive approaches. *See id*. at 13:24-34. The "summary" is inconsistent with the described embodiments, and therefore suffers from the same problem as claims 1 and 16 of the '544 patent. *See Baran v. Medical Device Techs., Inc.*, 616 F.3d 1309, 1316 (Fed. Cir. 2010) (dismissing reliance on "Summary of the Invention" section of specification where the Summary "simply repeats verbatim the claim language").

Columbia's reliance on the "Detailed Description of Exemplary Embodiments" is also misplaced. As Columbia notes, after describing the extraction of byte sequence features, the '544 and '907 patents state "[m]any additional methods of feature extraction are also useful." *See* Columbia Op. Br. at 11 (citing '544 patent at 6:23-25). As Columbia also notes, the patents then discuss the extraction of resource information. *See* Columbia Op. Br. at 11. Significantly, and contrary to Columbia's position, this section is describing "additional methods of ***feature*** extraction," ***not*** additional methods of ***byte sequence*** feature extraction. *See* '544 patent at 6:23-25. Columbia then argues, "the patent teaches that, when extracting a byte sequence feature from the executable, one of the pieces of information that must be included in certain embodiments is a 'byte string representative of resources referenced' by the executable." Columbia Op. Br. at 11.

The patents teach nothing of the sort. Rather, they describe the "resource information" or "binary profiling" feature extraction approach as an "alternative[]" to the byte sequence feature extraction approach that is "performed . . . in another embodiment." *See* '544 patent at 13:29-32; *see also* Dkt. No. 107-32 (Declaration of Trent Jaeger),¶¶ 22-24 ("The '544 patent is unequivocal that the 'byte sequence' feature extraction embodiment is separate and distinct from the 'resource information' or 'binary profiling' embodiment.").

Because claims 1 and 16 conflate two features that the specification describes as separate and distinct, they fail to inform persons skilled in the art about the scope of the invention with reasonable certainty, and are therefore indefinite under 35 U.S.C § 112, paragraph 2. *See Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S.Ct. 2120, 2129 (2014).

### C. <u>"email interface"</u>

| Symantec's Proposed Construction | Columbia's Proposed Construction |
|---|---|
| component that reintegrates filtered email back into normal email traffic | If the Court believes the term should be construed: hardware or software that interacts with email traffic and other email processing components |

The '544 patent and '907 patents describe the email interface as a system component with one constant purpose: to "reintegrate[] filtered email back into normal email traffic." *See* '544 patent at 15:30-34. Symantec's proposed construction comports with this description. *See Merck & Co., Inc. v. Teva Pharm. USA*, 347 F.3d 1367 (Fed. Cir. 2003) ("[C]laims must be construed so as to be consistent with the specification, of which they are a part.").

Neither the intrinsic record nor Columbia's proffered extrinsic evidence supports its construction. In fact, Columbia does not appear to rely on *any* intrinsic evidence for its construction. And Columbia cites only a single dictionary definition, not of "email interface," the term used in the '544 and '907 patents, but of "interface." *See* Columbia Op. Br. at 12-13. This definition reads "[s]ome form of electronic device that enables one piece of gear to communicate with or control another." *Id.* at 13. The definition does not support Columbia's construction, which contains no reference to the email interface "communicat[ing] with or control[ling] another" device or component.

With no evidence to support its construction, Columbia accuses Symantec of selectively importing only one of many disclosed functions of the email interface into its construction. *See id.* Not so. The '544 and '907 patents describe ***all*** the other disclosed functions of the email interface as optional. *See* '544 patent at 15:30-34 ("email interface 232 . . .which ***may s***end the model generator 240 . . . each attachment to be analyzed further") (emphasis added); *id.* at 15:35-

36 ("the email interface 232 ***may*** add warnings to the email or quarantine the email" (emphasis added); *id*. at 15:65-66 ("[t]he filter interface 242 ***may*** receive copies of all attachments from the email interface 232") (emphasis added). In contrast, the reintegration of filtered email back into normal email traffic is not described as optional. '544 patent at 15:30-34 ("email interface 232, which reintegrates filtered email back into normal email traffic 300.").

Columbia's reliance on *Generation II Orthotics* is inapposite. *See* Columbia Op. Br. at 13. First, that case involved a means-plus-function limitation, and the disputed term was the claimed function, "controlled medial and lateral inclination of each arm." *Generation II Orthotics Inc. v. Med. Tech. Inc.*, 263 F.3d 1356, 1363 (Fed Cir. 2001). In determining that the term should receive its plain and ordinary meaning, the Federal Circuit repeatedly emphasized that it would be improper to construe a functional term beyond the express claim language. *Id*. at 1364-65 ("When construing the functional statement in a means-plus-function limitation, we must take great care not to impermissibly limit the function by adopting a function different from that explicitly recited in the claim."). Here, the disputed term "email interface" is not part of a means-plus-function limitation; rather, it is a structural limitation. Thus, it is entirely appropriate to construe the term. *See Phillips*, 415 F.3d at 1311 ("While the baffles in the '798 patent are clearly intended to perform several functions, the term 'baffles' is nonetheless structural. … Accordingly, we must determine the correct construction of the structural term 'baffles,' as used in the '798 patent.").

Second, the Federal Circuit determined that "controlled" had a plain and ordinary meaning, and therefore did not require construction beyond the plain claim language. *See Generation II Orthodontics* at 1367. Here, neither party contends that "email interface" has a plain and ordinary meaning; rather, it is creature of the '544 and '907 patents, and can be understood only in the context of those patents. *See Phillips*, 415 F.3d at 1314 ("Because the meaning of a claim term as understood by persons of skill in the art is often not immediately apparent, and because patentees frequently use terms idiosyncratically, the court looks to those sources available to the public that show what a person of skill in the art would have understood disputed claim language to mean.") (internal quotations omitted).

Finally, *Generation II Orthodontics* was decided four years before *Phillips*, which cautioned against construing claim terms in a vacuum—especially terms that lack an plain and ordinary meaning—and emphasized the importance of the specification in determining the appropriate construction. *See Phillips*, 415 F.3d at 1315 ("The claims, of course, do not stand alone. … [T]he specification is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.") (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996) (internal quotations omitted). The Court should follow *Phillips*' guidance and construe the term "email interface" consistent with its description in the specification.

## III. <u>'084 AND '306 PATENTS</u>

### A. <u>"probabilistic model of normal computer system usage" / "normal computer system usage"</u>

| Symantec's Proposed Construction | Columbia's Proposed Construction |
|---|---|
| model of typical, attack-free, computer system usage that is based on probability / typical, attack-free, computer system usage | If the Court believes the term should be construed: "a model of normal computer usage that employs probability." Probability is "the likelihood that an event will occur or a condition will be present." |

***Model of Normal Computer System Usage.*** Columbia does not dispute that the term "normal" as used in the '084 and '306 patents means free of abnormalities, such as attacks or intrusions. *See* Columbia Op. Br. at 21 (distinguishing "normal activity" from "abnormal activity"); 22 (distinguishing "normal data" from "abnormal data"). Instead, Columbia argues that the claimed "model of ***normal*** computer system usage" may nevertheless include data representing abnormal usage. *See generally id*. at 20-23. Columbia's argument ignores that the claims explicitly require a "model ***of*** normal computer system usage"—not a model that simply includes normal usage data (among other things). Columbia's argument also ignores the intrinsic record's consistent explanation that a "model of normal computer system usage" is trained using clean or "attack-free" data, as detailed in Symantec's opening brief. *See generally* Symantec Op. Br. at 14-16. The Court should reject Columbia's argument for the following reasons.

***First***, Columbia's intention is to read the term "normal" out of the claimed "model of normal computer system usage." If successful, Columbia will argue that the asserted claims cover systems and methods that model and detect ***attack behavior***. This result would conflict with the invention's fundamental operation as an anomaly detection system. *See* '084 patent as 7:47-49 ("Anomaly detectors, such as anomaly detector 16, ***do not operate by looking for malicious activity directly***. Rather, they look for deviations from normal activity."). It would also allow Columbia the opportunity to read the claims on functionality it expressly distinguished in the specification and prosecution history. In particular, the specification contrasts the claimed invention from prior art systems that "detect the effects or behavior of malicious software rather than distinct signatures of that software." *See* '084 patent at 2:22-25. And during prosecution, the patentees distinguished the claimed invention from the cited Chong reference, which trains models using both normal and abnormal data to predict attacks that conform with attacks observed during training. *See* Dkt. No. 107-30 ('084 patent prosecution history) at COL00144299; *see also* Symantec Op. Br. at 15-16 (discussing prosecution history).[3]

[3] Columbia and its expert omit any discussion of prior art systems that include attack data in their models, instead focusing on the signature-based systems that have no real relevance (footnote continued)

By arguing for a "model of normal computer system usage" that includes abnormal data, Columbia is attempting to undo these distinctions over the prior art, and thereby broaden the claims to encompass subject matter that it did not invent. This is improper. *See Nystrom v. Trex Co., Inc.*, 424 F.3d 1136, 1145-46 (Fed. Cir. 2005) ("Broadening of the ordinary meaning of a term in the absence of support in the intrinsic record indicating that such a broad meaning was intended violates the principles articulated in *Phillips*.").

***Second***, the express claim language requires a "model of ***normal*** computer system usage." If the model were to include ***abnormal*** data, as Columbia proposes, it would no longer define "***normal*** computer system usage"; instead, it would it be a "mixture model" that defines "noisy" computer system usage. The terms "mixture model" and "noisy" are found directly in the intrinsic record; they are used by the inventors to describe models that include some abnormal data, as distinct from models that train on normal, *i.e.*, clean data:

> Traditional anomaly detection techniques focus on detecting anomalies in new data after training on normal (or clean) data. In this paper, we present a technique for detecting anomalies without training on normal data. We present a method for detecting anomalies within a data set that contains a large number of normal elements and relatively few anomalies. We present a mixture model for explaining the presence of anomalies in the data.

*See* Dkt. No. 107-12 (Eskin, *Anomaly Detection Over Noisy Data Using Learned Probability Distributions*) at Abstract. The named inventors chose to claim a model of "normal" computer system usage, not a "mixture model" or a model of "noisy" data. Columbia should not be allowed to rewrite the claims by arguing the "model of normal computer system usage" may nevertheless include abnormal data. *See K–2 Corp. v. Salomon S.A.*, 191 F.3d 1356, 1364 (Fed.

to the present dispute. *See, e.g.*, Columbia Op. Br. at 15. Also absent is any discussion of the prosecution history.

Cir. 1999) ("Courts do not rewrite claims; instead, we give effect to the terms chosen by the patentee.").

Using an apples-and-oranges analogy, Columbia's position is akin to arguing that a model of apples—which is used to detect oranges as a deviation from apples—may nevertheless include data about oranges to create the model of apples. If this model were applied to a random basket of apples and oranges, it would not detect any deviations because both apples and oranges would be part of the model. *See* Eskin at 1 ("If there is an intrusion hidden in the training data, the anomaly detection method will assume that it is normal and not detect subsequent occurrences."). To avoid such a result, the specification explains that a "model of normal computer system usage" is trained on attack-free data:

> Some attacks involve launching programs that have not been launched before and/or changing keys that have not been changed since the operating system was first installed by the manufacturer. ***If a model of the normal registry behavior is trained over clean data***, then these kinds of registry operations will not appear in the model, and can be detected when they occur.

'084 patent at 6:26-32.

The facts here are analogous to *Cat Tech LLC v. TubeMaster, Inc.*, 528 F.3d 871, 885 (Fed. Cir. 2008). In *Cat Tech*, the claims required "a spacing between adjacent plates having a width not greater than the smallest dimension of a single particle." *Id.* at 884. The patentee argued that the claim could be satisfied if the spacing requirement was met at a single "pinch point," even if the spacing requirement was not met at other points. *Id.* The district court disagreed and granted summary judgment of non-infringement, and the Federal Circuit affirmed. *Id.* at 885 ("Cat Tech's strained 'pinch point' construction of the phrase 'a spacing' renders an important claim limitation—the requirement that there be a spacing narrower than the width of a whole catalyst particle—functionally meaningless."). Here, if the claimed "model" can include abnormal or attack data, then the requirement that the model defines "***normal*** computer system usage" would be rendered effectively meaningless.

***Third***, Columbia's position relies on a mischaracterization of the claims. Columbia argues as follows:

> The claims specify that the "model of normal computer system usage" must ***include*** data on normal activity.

Columbia Op. Br. at 18 (emphasis added).

> The claims make clear that the "model of normal computer system usage" must ***use*** "records of normal processes that access the operating system registry," but the claims do not state that this is the only data that can be ***used*** to create the model.

*Id*. at 21 (emphasis added).

Contrary to Columbia's selective quotation, the claims require the "model of normal computer system usage" to be "***based on***" records of normal processes, not simply to ***use*** or ***include*** them:

> 1. A method for detecting intrusions in the operation of a computer system comprising:
>
> (a) gathering ***features from records of normal processes*** that access the operating system registry;
>
> (b) generating a probabilistic ***model of normal computer system usage*** ***based on the features*** and determining the likelihood of observing an event that was not observed during the gathering of features from the records of normal processes; and
>
> (c) analyzing features from a record of a process that accesses the operating system registry to detect deviations from normal computer system usage to determine whether the access to the operating system registry is an anomaly.

'084 patent at claim 1 (emphasis added). The emphasized language confirms that the claims require a "model of normal computer system usage" that is "based on" features of "normal processes." Columbia fails to explain how a model that includes abnormal data could satisfy these express requirements.

Columbia's reliance on *SunTiger* is therefore inapposite. Columbia Op. Br. at 21. That case involved a claim directed to an eyeglass lens made with a specific dye that "allows the lens to transmit" light at certain levels. *SunTiger, Inc. v. Scientific Research Funding Group*, 189 F.3d 1327, 1331 (Fed. Cir. 1999). The accused lenses included the claimed dye and allowed light to be transmitted at the claimed levels, but also included a gray coating that reduced light transmission below the claimed levels for all but the lower-right portion of the lenses. *Id.* On these facts, the Federal Circuit found that the accused lenses still could infringe if the lower-right portion met the claim language, *i.e.*, allowed transmission of light at the claimed levels. *Id.* at 1336 ("The district court's error lies in the fact that we have never required that a claim read on the entirety of an accused device in order to infringe.").

Here, by contrast, if a model includes abnormal data, it cannot be a "model of normal computer system usage"; instead, it becomes a "noisy model" or "mixture model" as discussed in the Eskin paper. Thus, where the lenses in *SunTiger* could still meet the claims despite the "gray coating," a model that includes abnormal data cannot meet the claims of the '084 and '306 patents because it no longer defines "normal computer system usage."

***Fourth***, there is not a single piece of intrinsic evidence to support Columbia's position that the claimed "model of normal computer system usage" may include abnormal data. Columbia first relies on a passage of the specification that says "other anomaly detection algorithms may also be used in connection with the present invention." Columbia Op. Br. at 21. It is unclear whether this statement refers to the "model" aspect of the invention, and notably Columbia cites the same language to support its argument that the specification discloses different embodiments of a "probabilistic model." *See id.* at 20. To the extent the statement does refer to models, it suggests that there may be other ways to determine if a particular observed activity is a deviation from a model of normal computer system usage; it does not suggest an embodiment of the "normal" model that includes abnormal data.

Indeed, the specification consistently defines the "model of normal computer system usage" as attack-free. *See generally* Symantec Op. Br. at 14-16. Columbia is wrong, therefore, to suggest that Symantec is attempting to limit the claims to a single embodiment. This is not an instance where the claims require a generic model and the specification discloses several embodiments of the model, one of which is "normal." Rather, the claim language is expressly limited to a "model of ***normal*** computer system usage," and Symantec has asked the Court to construe this term in accordance with its ordinary meaning in light of the specification.

Columbia is also wrong to rely on *Gemstar-TV Guide Int'l v. U.S. Int'l Trade Comm'n*, 383 F.3d 1352 (Fed. Cir. 2003). *See* Columbia Op. Br. at 22. There, the Federal Circuit was not considering the ordinary and customary meaning of the term "selection criteria," but instead was determining whether the patentees had disavowed criteria other than three specific examples in the specification. *See Gemstar*, 383 F.3d at 1378. Symantec is not arguing that Columbia disavowed "normal models that include abnormal data"; no such embodiment exists. Instead, Symantec is arguing that a person skilled in the art would understand the ordinary meaning of the term "model of normal computer system usage" in the context of the specification to exclude abnormal data, such as attacks. *See Medrad, Inc. v. MRI Devices Corp.*, 401 F.3d 1313, 1319 (Fed. Cir. 2005) ("We cannot look at the ordinary meaning of the term ... in a vacuum. Rather, we must look at the ordinary meaning in the context of the written description and the prosecution history.").

Next, Columbia cites column 2, lines 34-39, but fails to explain how this passage supports its position. *See* Columbia Op. Br. at 21-22. Indeed, the passage explains that anomaly detection systems detect attacks as ***deviations*** from a model of normal behavior, which supports

Symantec's position that the model must be attack-free in order to detect attacks as deviations. *See* '084 patent at 6:30-32 ("If a model of the normal registry behavior is trained over clean data, then these kinds of registry operations will not appear in the model, and can be detected when they occur.").

Finally, Columbia alleges that the Eskin paper is one of "a number of exemplary articles that construct models of normal behavior using data sets that include data on normal activity, but also supplement these models with data on abnormal activity." Columbia Op. Br. at 22. This statement mischaracterizes Eskin, which expressly distinguishes "normal" models based on attack-free data from "noisy" or "mixed" models that include some abnormal data, as discussed above. *See* Eskin at Abstract. Nowhere does Eskin disclose a "normal" model that includes abnormal activity as Columbia contends.[4] With nothing to point to in the intrinsic record, Columbia's "evidence" is nothing more than its conclusory expert declaration, which cannot contradict the clear intrinsic evidence. *See Phillips*, 415 F.3d at 1318 ("[C]onclusory, unsupported assertions by experts as to the definition of a claim term are not useful to a court. Similarly, a court should discount any expert testimony that is clearly at odds with the claim construction mandated by the claims themselves, the written description, and the prosecution history, in other words, with the written record of the patent.") (quoting *Key Pharms. v. Hercon Labs. Corp.*, 161 F.3d 709, 716 (Fed Cir. 1998) (internal quotations omitted); *see also SunTiger*, 189 F.3d at 1335-36 ("[T]he language of the patent itself leaves no real doubt regarding the

[4] Columbia's brief does not address any other "exemplary articles," but instead refers to its expert declaration. *See* Columbia Op. Br. at 22. Paragraphs 67-70 of the declaration mischaracterize the other "exemplary articles" in the same way that Columbia's brief mischaracterizes Eskin. *See* Szajda Decl. ¶¶ 67-70. Not a single cited article discloses a "normal" model that includes abnormal activity, and Dr. Szajda's selected quotations from the articles confirm this. *See id*.

proper claim construction … there is no need for, and it would be improper for us to rely upon, the extrinsic evidence offered by SunTiger.”).

***Probabilistic Model***.[5] The parties’ dispute concerns whether a “probabilistic model” is one that is “based on probability,” as Symantec proposes, or one that “employs probability,” as Columbia proposes. Symantec’s interpretation is the plain meaning of the term as it would have been understood at the time of the invention. *See* Declaration of Nathan Hamstra in Support of Symantec’s Responsive Claim Construction Brief (Hamstra Responsive Decl.), Ex. 1 (The Oxford American College Dictionary, 2002 Ed.) at 1082 (“probabilistic: based on or adapted to a theory of probability.”).[6] *See Phillips*, 415 F.3d at 1322 (“Dictionaries or comparable sources are often useful to assist in understanding the commonly understood meaning of words.”). Symantec’s proposal is also consistent with the plain language of the claims, which uses the term “probabilistic” to describe what the model ***is*** (*i.e.*, based on probability), not what it ***does*** (*i.e.*, employ probability).

### B. “anomaly” / “anomalous”

| Symantec’s Proposed Construction | Columbia’s Proposed Construction |
|---|---|
| deviation from a model of typical, attack-free behavior / deviating from a model of typical, attack-free behavior | If the Court believes the term should be construed: behavior that deviates from normal and may correspond to an attack. |

Anomaly detection systems, such as those described in the ‘084 and ‘306 patents, detect

[5] Columbia’s opening brief addresses a construction for “probabilistic” that Symantec withdrew during the parties’ exchange of proposed constructions—“based on a probability density function.” *See* Columbia Op. Br. at 17-18. As stated in its opening brief, Symantec’s position is that Columbia waived the right to construe “probabilistic,” but if the Court believes construction is necessary, the term should receive its plain meaning, “based on probability.” *See* Symantec Op. Br. at 13 n. 6.

[6] Extrinsic evidence is necessary in this instance because the specification does not define a plain and ordinary meaning of the term “probabilistic.”

anomalies as deviations from a model of normal behavior. This is apparent from the plain language of the claims, which use a model to define "normal computer system usage," and then detect deviations from "normal computer system usage" to identify "an anomaly":

> 1. A method for detecting intrusions in the operation of a computer system comprising:
>
> (a) gathering features from records of normal processes that access the operating system registry;
>
> (b) generating a probabilistic ***model of normal computer system usage*** based on the features and determining the likelihood of observing an event that was not observed during the gathering of features from the records of normal processes; and
>
> (c) analyzing features from a record of a process that accesses the operating system registry ***to detect deviations from normal computer system usage*** to determine whether the access to the operating system registry is ***an anomaly***.

'084 patent at claim 1 (emphasis added).

The fact that an anomaly is understood to be a deviation from a model of normal behavior is also apparent from the intrinsic evidence, including the evidence Columbia cites in its opening brief. *See* Columbia Op. Br. at 23; *see also* '084 patent at 2:34-37 ("Anomaly detection algorithms may build ***models*** of normal behavior in order to detect behavior that deviates from normal behavior and may correspond to an attack."); *id*. at 3:17–30 ("It is another object of the invention to generate a ***model*** of the normal access to the Windows registry, and to detect anomalous accesses to the registry that are indicative of attacks."); *id*. at (emphasis added)*; id*. at 7:48–49 (referring to "anomaly detector 16"); *id*. at 5:16-18 ("The ***model*** is then used by the anomaly detector 16 to decide whether each new registry access should be considered anomalous."). The Court should construe the terms "anomaly" and "anomalous" consistent with their use in the claims and specification. *See Phillips*, 415 F.3d at 1316-17 ("It is therefore entirely appropriate for a court, when conducting claim construction, to rely heavily on the written description for guidance as to the meaning of the claims.”).

### C. “operating system registry”

| Symantec’s Proposed Construction | Columbia’s Proposed Construction |
|---|---|
| database of information about a computer’s configuration | If the Court believes the term should be construed: a database of information about a computer’s configuration, utilized by an operating system, organized hierarchically as a tree, with entries consisting of keys and values |

In its opening brief, Columbia argues that Symantec’s construction “excises” certain parts of the specification’s description of an “operating system registry.” But it is actually Columbia’s proposed construction that does this, notably omitting the specification’s description of the registry as “the storage location for all security information such as security policies, user names, and passwords.” ‘084 patent at 5:31-33.[7] As a result, Columbia’s construction is based on selectively importing limitations describing a particular embodiment of a registry from the specification into the claims, which Columbia admits is improper. *See* Columbia Op. Br. at 3 (“As the court explained in Phillips, ‘if we once begin to include elements not mentioned in the claim, in order to limit such claim . . . we should never know where to stop.”) (citing *Phillips*, 415 F.3d at 1312). Symantec’s construction, on the other hand, focuses on the general definition of an operating system registry provided in the specification, without arbitrarily importing select limitations from a specific embodiment of a registry into the claims.

Columbia’s remaining arguments rely entirely on extrinsic evidence, including its expert declaration and two articles that are not cited in the ‘084 and ‘306 patents or prosecution histories. *See* Columbia Op. Br. at 16-17. The Court should disregard this evidence, especially

[7] Columbia’s brief omits this sentence from its block quote of the specification. *Compare* Columbia’s Opening Br. at 16 *with* ‘084 patent at 5:21-38.

in light of the specification's clear description of a registry as a "database of information about a computer's configuration."

## IV. '115 AND '322 PATENTS

### A. "emulator"

| Symantec's Proposed Construction | Columbia's Proposed Construction |
|---|---|
| software, alone or in combination with hardware, that simulates a computer system | software, alone or in combination with hardware, that permits the monitoring and selective execution of certain parts, or all, of a program |

A wealth of intrinsic and extrinsic evidence confirms that an emulator is software, alone or in combination with hardware, that simulates a computer system. *See generally* Symantec Op. Br. at 24-26.[8] Columbia's proposed construction does not seek to define what an "emulator" is, but rather defines "emulator" as selected tasks that disclosed embodiments use an emulator to perform. This approach is logically flawed. That an emulator may be used to perform certain tasks does not imply that any software used to perform the tasks is an emulator.

The intrinsic evidence plainly supports Symantec's construction. The '115 and '322 patents state that emulated "instructions [are] executed by the virtual processor." *See* Dkt. No. 107-13 ('115 patent) at 13:61-14:5. Similarly, U.S. Provisional Application No. 60/730,289, which the '115 and '322 patents incorporate by reference, explains that the "emulator . . . executes all instructions on the virtual processor." *See* Dkt. No. 107-14 ('289 application) at

[8] Rather than addressing Symantec's proposed construction on the merits and in light of the intrinsic record and extrinsic evidence, Columbia repeatedly dismisses it as simply replacing the word "emulator" with "simulator." *See* Columbia Op. Br. at 27. This argument misrepresents Symantec's construction. Symantec's proposal is "software, alone or in combination with hardware, that simulates a computer system," not "simulator." Thus, Symantec does not simply replace "emulator" with "simulator," but instead defines precisely what the emulator simulates, consistent with the intrinsic record and extrinsic evidence.

COL00007628. And prior art references cited before the U.S. Patent & Trademark Office during prosecution of the '115 and '322 patents define "emulation" as "running a computer program in a simulated environment rather than in a real environment." *See* Dkt. No. 107-16 (U.S. Patent No. 5,978,917) at 2:42-44; *see also* Dkt. No. 107-17 (U.S. Patent No. 6,952,776) at 7:9-12 (referring to a "program-emulation step that executes the current object in a virtual environment").

The extrinsic evidence likewise supports Symantec's construction. Persons of ordinary skill in the art at the time of the invention would have understood the term "emulator" to require the execution of a program in a simulated environment. *See* Dkt. No. 107-1 (Declaration of Richard Ford), ¶¶ 12-14. Contemporaneous dictionaries and treatises in the field of software development and computer security describe emulators in the same way. *See* Symantec Op. Br. at 25; *see also* Dkt. Nos. 107-20 to 107-23 (providing example definitions from dictionaries and treatises).

Columbia's arguments rely on descriptions, not of what an emulator is, but how various disclosed embodiments use the emulator. For instance, Columbia relies on a quote from the specification that states, "The use of an emulator allows the system to detect and/or monitor a wide array of software failures." *See* Columbia Op. Br. at 28 (quoting '115 patent at 14:16-19, 13:54-61). But this portion of the specification does not define "emulator"—it merely describes the purpose for which a certain disclosed embodiment uses an emulator.

Columbia also erroneously states that the disclosed "STEM" embodiment is an "emulator," selectively quoting the patent specification. *See* Columbia Op. Br. at 28 ("STEM, a preferred embodiment emulator, 'permits the selective execution of certain parts, or all, of a program.'") (quoting '115 patent at 3:28-33). The full quote makes clear that STEM is not an "emulator," but rather only one way to ***use*** an emulator:

> In various embodiments, using PAD to model program stack information, such stack information may be extracted using, for example, Selective Transactional EMulation (STEM), which is described below and which permits the selective execution of certain parts, or all, of a program ***inside an instruction-level emulator, using the Valgrind emulator***.

'115 patent at 3:28-33 (emphasis added).

Thus, Columbia's attempt to define "emulator" as the disclosed STEM embodiment is wrong according to the express language of the '115 and '322 patents. In fact, the intrinsic evidence defines Valgrind, the emulator used by STEM, consistent with Symantec's proposed construction of "emulator." *See* Hamstra Responsive Decl., Ex. 2 (Barrantes et al., *Randomized Instruction Set Emulation to Disrupt Binary Code Injection Attacks*) at COL00007905 ("Valgrind ***simulates*** the operation of the CPU.") (emphasis added); *see also* Hamstra Responsive Decl., Ex. 3 ('322 patent prosecution history, citing Barrantes et al.) at 3.

### B. "anomalous"

| Symantec's Proposed Construction | Columbia's Proposed Construction |
|---|---|
| deviating from a model of typical, attack-free computer system usage | If the Court believes the term should be construed: behavior that deviates from normal and may correspond to an attack |

Anomaly detectors identify behavior as anomalous by building a model of normal behavior, and then comparing subsequently observed behavior to see if it deviates from the model of normal behavior. *See, e.g.*, '115 patent at 3:50-56. The provisional application to which the '115 and '322 patents claim priority agrees: "Anomaly detection algorithms build models of normal behavior in order to detect behavior that deviates from normal." *See* Dkt. No. 107-14 ('289 application) at COL00007613. Columbia ignores this intrinsic evidence, arguing that (1) "deviations from normal" may be detected without a comparison to normal, and (2) "normal" does not mean "normal," but instead means "normal and attacks." The Court should reject both arguments.

Regarding the first dispute, the plain language of the asserted claims confirms that "anomalous" function calls are those that deviate from a model of normal function calls:

> 1. A method for detecting anomalous program executions, comprising:
>
> executing at least a part of a program in an emulator;
>
> ***comparing a function call made in the emulator to a model of function calls*** for the at least a part of the program;
>
> ***identifying the function call as anomalous based on the comparison***; and
>
> upon identifying the anomalous function call, notifying an application community that includes a plurality of computers of the anomalous function call.

'115 patent at claim 1 (emphasis added). The emphasized language demonstrates that a function call is identified as "anomalous" based on a comparison with a model. *See id*. And, as Columbia agrees, "anomalous" behavior is behavior that deviates from normal. *See* Columbia Op. Br. at 25 ("An anomaly is that which deviates from normal."). It follows, then, that the model claimed in the '115 and '322 patents must model normal function calls in order to identify "anomalous" behavior, *i.e.*, behavior that deviates from normal. That is precisely how anomaly detection systems work: they "build models of normal behavior in order to detect behavior that deviates from normal." *See* '289 application at COL00007613.

Columbia relies on the doctrine of claim differentiation to argue that requiring normal activity in the independent claim is improper. *See* Columbia Op. Br. at 26. But the dependent claim on which Columbia relies does not merely recite "normal activity"; instead, it recites "normal activity ***for at least a portion of the program***." *See* '322 patent at claim 6 (emphasis added). Symantec's proposed construction would not render this language redundant, and thus the Court should reject Columbia's claim differentiation argument. *See Edwards Life Sciences, LLC v. Cook, Inc.*, 582 F.3d 1322, 1330-32 (Fed. Cir. 2009) (declining to apply claim differentiation where it did not render claim language redundant, and further recognizing that "claim differentiation is a rule of thumb that does not trump the clear import of the specification.").

The second dispute is whether a model of normal behavior is a model of normal behavior or a model of normal behavior as well as attack behavior. As set forth above in the discussion of the '084 and '306 patents, normal models are models consisting of normal data, *i.e.*, data that is free of attacks. The '115 and '322 patents confirm this plain and ordinary meaning, and fail to describe any embodiment that employs a normal model that nevertheless includes attack data. *See* '115 patent at 3:50-57. Likewise, the '289 application confirms that a normal model trains on normal data. *See* '289 application at COL00007615 (describing training over "clean data"); *id*. at COL00007605 (describing training on "attack-free records").

### C. "application community"

| Symantec's Proposed Construction | Columbia's Proposed Construction |
|---|---|
| members of a community running the modeled program | If the Court believes the term should be construed: members of a community running the same program or a selected portion of the program |

The parties appear to agree that an application community means members of a community running the program that is being monitored, *i.e.*, the claimed "program" that is executed in the emulator. *See* '115 patent at claim 1 ("executing at least a part of a program in an emulator."). The parties have two disputes. First, Columbia seeks to insert a requirement that the community is running the program or only a "selected portion of the program." Second, Symantec seeks to describe that, consistent with the language of the claims, the program the members of the community run is the program that is modeled. *See id*. ("comparing a function call made in the emulator to a ***model*** of function calls ***for the at least a part of the program***."). The Court should adopt Symantec's proposed construction.

The structure of the claims supports Symantec's proposed construction. The phrase "the … program" in Symantec's proposed construction and the phrase "the program" in Columbia's proposed construction both necessarily refer back to the antecedent "program" in the phrase "executing at least a part of a program in an emulator," as well as "the program" included in the phrase "comparing a function call made in the emulator to a model of function calls for the at least a part of the program." *See* '115 patent at claim 1. It follows that "application community" refers to members of a community running the program for which there is a "model of function calls," *i.e.*, the modeled program.

Columbia's importation of a limitation from "certain embodiments" of the "application community" lacks support in law or fact. Columbia states that the "specification also makes clear that in ***certain embodiments*** any one member of the community may only monitor a portion of the program." Columbia Op. Br. at 30 (emphasis added). But Columbia does not provide any basis for limiting the claims to those "certain embodiments." This language Columbia seeks to import into the claims is also superfluous and therefore potentially confusing to a jury. A member of the community that is "running a selected portion of the program" is still running "the program."

## V. **CONCLUSION**

For the foregoing reasons, Symantec respectfully requests that the Court adopt its proposed constructions.

August 28, 2014

SYMANTEC CORPORATION

By:
/s/
Of Counsel

Dabney J. Carr, IV, VSB #28679
TROUTMAN SANDERS LLP
P. O. Box 1122
Richmond, Virginia 23218-1122
Telephone: (804) 697-1200
Facsimile: (804) 697-1339
dabney.carr@troutmansanders.com

David A. Nelson (*pro hac vice*)
davenelson@quinnemanuel.com
Stephen A. Swedlow (*pro hac vice*)
stephenswedlow@quinnemanuel.com
Nathan A. Hamstra (*pro hac vice*)
nathanhamstra@quinnemanuel.com
500 West Madison St., Suite 2450
Chicago, Illinois 60661
Telephone: (312) 705-7400
Facsimile: (312) 705-7401
QUINN EMANUEL URQUHART &
SULLIVAN LLP

Derek L. Shaffer (*pro hac vice*)
derekshaffer@quinnemanuel.com
777 6th Street NW, 11th floor
Washington, D.C. 20001-3706
Telephone: (202) 538-8000
Facsimile: (202) 538-8100
QUINN EMANUEL URQUHART &
SULLIVAN LLP

*Attorneys for Defendant*
*Symantec Corporation*

## CERTIFICATE OF SERVICE

I hereby certify that on this 28th day of August, 2014, I electronically filed the foregoing pleading with the Clerk of Court using the CM/ECF system, which then will send automatic notification of such filing (NEF) to the following:

Dana Duane McDaniel (dmcdaniel@spottsfain.com)
John Michael Erbach (jerbach@spottsfain.com)
Spotts Fain PC
411 E Franklin St, Suite 600
PO Box 1555
Richmond, VA 23218-1555
(804) 697-2065
Fax: (804) 697-2165

David I. Gindler (*pro hac vice*)
dgindler@irell.com
Jason G. Sheasby (*pro hac vice*)
jsheasby@irell.com
Richard M. Birnholz (*pro hac vice*)
rbirnholz@irell.com
Crawford Maclain Wells (*pro hac vice*)
mwells@irell.com
Thomas C. Werner (*pro hac vice*)
twerner@irell.com
Gavin Snyder (*pro hac vice*)
gsnyder@irell.com
Douglas Allen Fretty (*pro hac vice*)
dfretty@irell.com
IRELL & MANELLA LLP
1800 Avenue of the Stars
Los Angeles, CA 90067
Phone: (310) 277-1010
Fax: (310) 203-7199

Michael Henry Strub, Jr. (*pro hac vice*)
mstrub@irell.com
IRELL & MANELLA LLP
840 Newport Center Drive
Newport Beach, CA 92660
Phone: (949) 760-0991
Fax: (949) 760-5200

*Counsel for The Trustees of Columbia University*
*In the City of New York*

/s/
Dabney J. Carr, IV, VSB #28679
TROUTMAN SANDERS LLP
P. O. Box 1122
Richmond, Virginia 23218-1122
Telephone: (804) 697-1200
Facsimile: (804) 697-1339
dabney.carr@troutmansanders.com

*Counsel for Defendant Symantec Corporation*